ランサムウェア対策事例

みやぎ県南中核病院 様

AIを活用して不審な通信を検出
セキュリティインシデントを早期発見

みやぎ県南中核病院
副院長
統合情報診療部長
放射線診断科 主任部長
医学博士
清治 和将 氏

みやぎ県南中核病院
統合情報診療部
医療情報管理課　課長
坂野 隆明 氏

みやぎ県南中核病院
統合情報診療部
医療情報管理課　係長
遠藤 明義 氏

お客様名：みやぎ県南中核病院
所 在 地：宮城県柴田郡大河原町字西38−1
概　　要：仙南地域を中心に宮城県南部の広域をカバーする急性期病院。大河原町、柴田町、村田町、角田市の1市3町を経営母体として2002年に開院。33診療科、病床数310床、職員数は705人でこのうち医師は研修医を含めて110人（2024年4月）。特に急性期医療に力を入れており、敷地内にはドクターヘリ発着用のヘリポートを備えるなど救命救急センターを有する県内有数の救急医療施設として質の高い医療を提供している。

＜事例のポイント＞

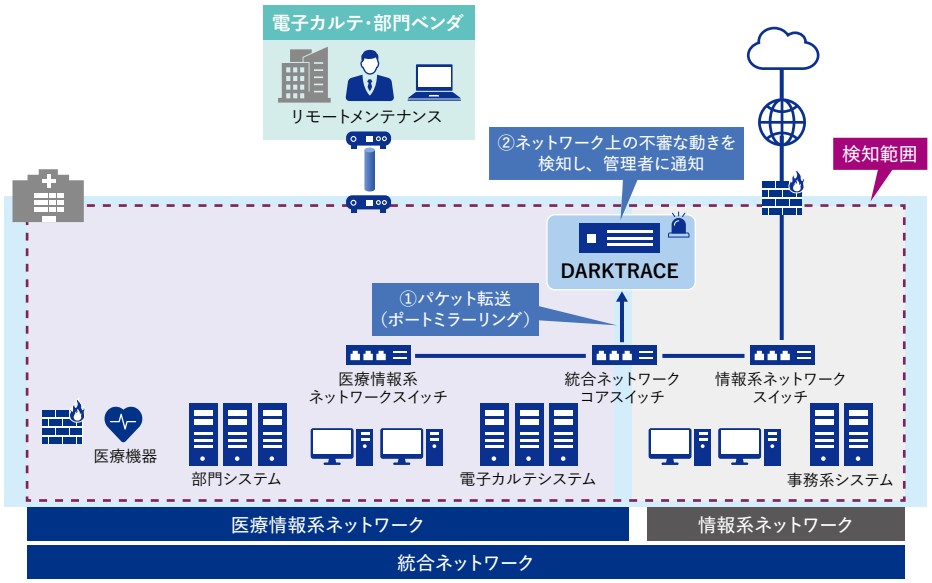
課題背景

- ネットワーク接続が増加し、不正な通信の検知の重要性が向上
- ネットワーク内に流れる異常なパケットの検知と一次対応の迅速化
- ランサムウェアの早期発見を実現するセキュリティ強化

成　　果

- NDR製品を導入することで端末間の不正通信の可視化が実現
- AIを活用したパケットの状況把握・分析により、スピーディな一次対応を実現
- ランサムウェアの早期発見を実現し、シャドーITへの対策に期待

● NDR導入後のネットワーク構成図



NEC　\Orchestrating a brighter world

NECフィールディング

〈導入の背景や課題〉 業務継続性を確保するためNDR導入を決断

サイバー攻撃はデジタルテクノロジーの進化により巧妙化、高度化しています。近年では情報ネットワークに侵入し身代金を要求するランサムウェアの被害も拡大し、企業だけでなく医療機関なども攻撃対象になっています。中には電子カルテシステムがランサムウェアの攻撃を受け、手術の中止や救急および一般外来の受け入れ制限などの事態に陥る病院もあります。

みやぎ県南中核病院様は、宮城県南部の急性期病院として日々多くの救急患者を受け入れています。副院長の清治和将氏は「サイバー攻撃で病院機能が停止すれば、救急車の受け入れができず、周辺医療機関との連携にも支障が出ます」と語り、業務停止を未然に防ぐ上でサイバーセキュリティ対策は重要だと考えています。

院内のネットワーク環境を管理する統合情報診療部医療情報管理課課長の坂野隆明氏は、「ウイルス対策ソフトなどエンドポイント対策は導入しています。しかしセキュリティを強化するために、どんなパケットが流れているかなどネットワーク対策の必要性を感じていました」と話します。院内はパソコンなどの端末だけでなく、ネットワークに接続する医療機器の台数も増えており、事後対策の必要性が高まっています。

増え続ける端末や医療機器に対してセキュリティチェックをするのは多大な労力がかかります。医療情報管理課係長の遠藤明義氏も「端末やネットワークにトラブルが発生すると、医療情報管理課への問い合わせが増えます。スタッフは多くないので対応の遅れも懸念されます」と、ネットワーク監視の必要性を感じていました。坂野課長は、「ネットワークの中を流れるパケットを見ることはできません。しかしそれを可視化することで、いち早く異常を検知しスピーディな対応につながります」との判断からNDR導入に向けた予算確保に乗り出しました。

〈選択のポイント〉 効果検証を経て本格導入へ　製品の機能に加えサポート体制も重視

坂野課長はNDRに関する情報収集を開始するとともに、ベンダにも問い合わせをして比較検討を行いました。その結果、ネットワークの異常挙動を検知するAI機能を搭載した「Darktrace(ダークトレース)」の導入が決まりました。

Darktraceは自己学習型のAIを搭載していることが特徴です。ネットワークを流れるパケットを監視しながら、通常では発生しないパケットなどの異常を検出しアラートを上げます。それをチェックして、そのパケットが異常なのか、そうではないのかを判断することでネットワークの健全性が担保される仕組みを構築できます。

NDR導入に当たっては、NECフィールディングは現行環境を加味した提案を行いました。NECフィールディングはみやぎ県南中核病院様が開院した当初からネットワークの保守・運用管理を担っており、院内のセキュリティ対策も熟知しています。坂野課長は「我々が検討していたNDR製品と、NECフィールディングが提案してくれたNDR製品が同じ製品でした」としつつ、日ごろから保守運用を任せているNECフィールディングの勧めなら、と安心してDarktraceを導入できたと語ります。

みやぎ県南中核病院様がNDR製品の導入を決めたのは、2023年秋のことです。導入に当たっては「比較的高価な製品なので、次年度の予算を確保することに苦心しました。他院のセキュリティ被害なども交えつつ経営層に説明しました」(坂野課長)。その根幹にあったのが、急性期病院としての使命感です。坂野課長は「当院の業務が止まってしまえば救急患者を遠方の病院まで搬送しなければならず、患者の命にもかかわります」と強調します。

Darktraceを本格導入する前には１カ月間の効果検証を行い、その結果を分析・評価しました。導入前に効果検証・評価ができたことで導入後の運用イメージを高められ、安心して導入できたそうです。

〈導入の成果〉 導入直後の効果は期待以上　今後は職員のITリテラシー向上が鍵に

Darktraceの導入支援をNECフィールディングに委託した理由に関して坂野課長は、「導入に際しては院内の電子カルテに影響が出ないようにする必要があります。日ごろからネットワークの保守・運用を任せているNECフィールディングであれば安心だと思い、お願いしました」と語ります。

効果検証期間を経て、2024年6月からDarktraceの本格運用が始まりました。導入効果について、「思ったよりネットワークの中を流れるパケットを可視化できたので、期待以上の効果がありました」(坂野課長)としています。さらに「DarktraceのAI学習データがどんどん大きくなっているのを見て、相当なパケットが流れているということが実感できるようになりました」と、ネットワーク可視化の効果を語ります。

今後の課題として坂野課長は、外部から持ち込まれる検査や画像などのデータの安全性確保や、医師などが医療データを活用するためにネットワークに接続してくるシャドーIT対策を挙げます。「まだ必要な対策は残っています。NECフィールディングからの情報提供を受けつつ、セキュリティ強化を推進していきたいです」と方針を示しています。また、遠藤係長によれば、「院内には多くの診療科があり、それぞれ専門とする分野も異なります。そのためセキュリティをはじめITに関する問い合わせも多岐にわたります」と現状を示した上で、職員のITリテラシー向上は急務だと語ります。みやぎ県南中核病院様では、職員のITリテラシー向上のための研修を年に1回実施しています。2024年からは年2回に増やし、そのうち1回は個人情報を含めた情報管理の研修会、もう1回はサイバーセキュリティを中心にした研修会としています。職員数が多いため、集合型研修だけでなくeラーニングでも受講できるようにしました。

医療DXの推進は政府の施策でもあります。「医療現場ではデジタル化は進んでいますが、医療連携を考えれば、地域の開業医などとの情報連携は進んでいません。長年のアナログ体質から抜け出すために、制度や業務の改革にも注目する必要があると考えます」と清治副院長は話しています。医療の地域連携には、中核となる病院や連携する医療機関のIT活用による医療DX強化が不可欠です。みやぎ県南中核病院様が進めるさまざまな施策の一助となるべく、NECフィールディングもさらなるサポートを続けていきます。

お問い合わせは、下記へ
NECフィールディング

デジタルビジネス統括部　医療SLグループ
URL：https://www.fielding.co.jp
E-mail：medical-ss@fildg.jp.nec.com

NEC \Orchestrating a brighter world

NECフィールディング株式会社　〒108-0023 東京都港区芝浦四丁目9番25号(芝浦スクエアビル)

2024年12月現在　CN2024-092(Rev.1.0)　有効期限 2026.11.30